

ORIGINAL

SUPERIOR COURT
YAVAPAI COUNTY, ARIZONA

2008 AUG 21 PM 4:53 ✓

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF YAVAPAI

BY: B. Hamilton

THE STATE OF ARIZONA,)
)
Plaintiff,)
)
vs.)
)
STEVEN CARROLL DEMOCKER,)
)
Defendant.)

No. CR 2008-1339

BEFORE: THE HONORABLE THOMAS B. LINDBERG
JUDGE OF THE SUPERIOR COURT
DIVISION SIX
YAVAPAI COUNTY, ARIZONA

PRESCOTT, ARIZONA
TUESDAY, JANUARY 13, 2009
4:19 P.M.

REPORTER'S TRANSCRIPT OF PROCEEDINGS

SIMPSON HEARING

TESTIMONY OF MARK CARDWELL

ROXANNE E. TARN, CR
Certified Court Reporter
Certificate No. 50808

JANUARY 13, 2009
4:19 P.M.

SIMPSON HEARING

APPEARANCES:

FOR THE STATE, MR. MARK AINLEY.
FOR THE DEFENDANT, MR. JOHN SEARS.

THE COURT: We are continuing CR 2008-1339,
State versus Steven Democker. Mr. Democker is present.
Mr. Sears is here. Mr. Ainley on behalf of the State.

Mr. Sears.

MR. SEARS: I would call Mark Cardwell, please

THE CLERK: Do you solemnly swear upon penalty
of perjury the testimony you are about to give will be the
truth, the whole truth, and nothing but the truth, so help
you God?

THE WITNESS: Yes, I do.

THE COURT: Will you please spell your last
name for our court reporter.

THE WITNESS: C-a-r-d-w-e-l-l.

MARK CARDWELL,
called as a witness, having been duly sworn, testified as
follows:

DIRECT EXAMINATION

BY MR. SEARS:

Q. Thank you for waiting, Mr. Cardwell. It has been
a long day.

1 Would you tell us what you do for a
2 living, please.

3 A. I am a computer forensic examiner. I have a
4 company that does forensic examinations for litigation.

5 Q. The name of the company is?

6 A. Forentech.

7 Q. Where is it located?

8 A. In Phoenix.

9 Q. How long have you been a principal at Forentech?

10 A. Since about 2001.

11 Q. Can you give Judge Lindberg a description of your
12 education and training and experience in computer forensics.

13 A. My educational background is a standard BS in
14 economics, Master of Business Administration with a focus in
15 technology.

16 My training in forensics includes course
17 work at Guidance Software, which develops a prominent product
18 in forensics, and at Access Data, which developed another
19 prominent product for forensics.

20 Q. What about on-the-job and practical experience,
21 particularly since you formed Forentech a number of years
22 ago? What does your work consist of?

23 A. My work primarily is commercial litigation in all
24 flavors of practice area. I have probably done on the order
25 of -- I don't know -- 6- or 700 hard drives. Something along

1 those lines.

2 Q. Analyzing data contained on hard drives that are
3 connected to civil or criminal litigation?

4 A. Yes. Hard drives, cameras --

5 Q. In front of you are two exhibits. One of them,
6 Exhibit 75, looks like it might be your current CV. Does
7 that look familiar to you?

8 A. Yes, it is.

9 Q. You provided that to us in connection with your
10 work in this case?

11 A. I did.

12 Q. And it accurately and currently reflects both your
13 education and training and experience?

14 A. It does.

15 MR. SEARS: Thank you. I would move
16 Exhibit 75.

17 MR. AINLEY: No objection.

18 THE COURT: 75 is admitted.

19 BY MR. SEARS:

20 Q. Now, can we talk a little bit about the work that
21 you've done in this case. You obviously were retained by my
22 firm to do an analysis of -- beginning with one particular
23 computer hard drive; is that right?

24 A. That's right.

25 Q. And arrangements were made to get you a copy or a

1 clone of the hard drive from a laptop computer that was
2 seized by the police in connection with this case; is that
3 right?

4 A. More specifically or more accurately, a
5 computer-forensic image created with Guidance EnCase
6 Software.

7 Q. And when I understate or overstate the point of
8 computer forensics, feel free to comment.

9 So can you tell us if you recall when you
10 were given or provided this forensic image?

11 A. That would have been a week ago Sunday.

12 Q. It was delivered to you in Phoenix?

13 A. Yes.

14 Q. And can you describe for Judge Lindberg what you
15 began to do in this case, and particularly whether you were
16 given any instructions or any requests from us with respect
17 to what we were asking you to do with this image.

18 A. Initially what I did was take the forensic image
19 that was captured by the sheriff's department or by the
20 police lab -- I am not sure who. I copied that onto my
21 network at Forentech for analysis, stored the original image
22 in secure storage, and then created an additional backup copy
23 on my backup server, which also contains copies of any
24 analysis work that I do on that image.

25 My direction has been relatively broad at

1 this stage. What I have been doing for the last week is
2 gathering a wide variety of data of all types to move forward
3 with analysis, once we have all that collection of data.

4 Q. And were you given any information about any
5 aspect of this case -- what the allegations are, what
6 relevance, if any, this laptop computer might have to the
7 case?

8 A. Only in broad terms. The only specific
9 information I have is the police report.

10 Q. And when you say "the police report," which report
11 are you talking about?

12 A. What was referred to as an "EnCase report,"
13 written, I think, by Detective Page.

14 Q. That was a document that was generated,
15 apparently, in connection with some forensic investigation he
16 had done with this same drive?

17 A. Yes. And it looks to be a result of a keyword
18 search, and it's just really, in essence, a listing of files.

19 Q. And you talk about EnCase. Can you describe for
20 Judge Lindberg what this EnCase program is and what it is
21 intended to do.

22 A. EnCase is a very technical product that was
23 developed by a company called Guidance Software, a company
24 which was built by former law enforcement people, for the
25 most part. Its purpose is to be able to create a safe

1 forensic image of an evidence hard drive without touching
2 that hard drive -- without -- that is, without making any
3 changes to it.

4 Once that image is made, the original
5 hard drive can be put away, and EnCase or other products are
6 then used to study the image, and in all respects it is
7 identical to the original evidence drive.

8 Q. Was actually the image that you were given to work
9 with apparently created with the EnCase Software?

10 A. That's right.

11 Q. And is this the same software outfit that you said
12 that you had training with, the people that produced EnCase?

13 A. Yes.

14 Q. So you have had specific training with the people
15 that developed the software about how to use it and how to
16 work with it in your work?

17 A. That's right.

18 Q. Now, if we can shift gears for a minute here and
19 talk about your experience in cases where law enforcement
20 had taken possession of or seized computers.

21 And from our discussions, I come away
22 with the impression that when the police come upon a running
23 computer -- one that is powered up and running -- that there
24 is a certain standard -- maybe even an industry standard --
25 for how the police are to best approach and deal with that

1 computer. Am I right?

2 A. Yes, there is.

3 Q. What is your understanding and the basis for your
4 understanding of what the police are supposed to do if they
5 want to preserve the integrity of a running computer?

6 A. Well, generally speaking, the protocol for seizing
7 a computer is the same whether it is in law enforcement or in
8 the private sector. And that is if the computer is running,
9 you deprive it suddenly of power. You do not want to do a
10 graceful shutdown of a Windows machine, because it can be
11 very destructive of data. So typically, you will just pull
12 the plug.

13 If it's a laptop computer, pulling the
14 plug doesn't do anything, because they run on batteries. So
15 the next step would be pulling the battery to suddenly
16 deprive it of power.

17 Q. Without touching any of the keys or opening or
18 closing the lid?

19 A. That's right.

20 Q. Now, a laptop computer, particularly an IBM laptop
21 computer like the one we are talking about here, has a number
22 of different levels or modes of activity. Am I describing
23 that correctly?

24 A. No. I don't think I understand the question.

25 Q. States of consciousness.

1 A. Okay. I understand.

2 Are you finished?

3 Q. I am.

4 A. I think what you are getting at is that a machine
5 can be running but still be in various states. One state
6 could be the typical work state where you're seeing things on
7 the screen there doing work.

8 Another state might be where you walk
9 away from it for 10 or 15 minutes and it goes to sleep. The
10 screen may go blank to preserve power. The hard drive may
11 stop spinning.

12 The next step is typically called
13 "hibernation," and that's where it goes into, basically, as
14 deep a power preservation mode as possible and draws very,
15 very little power from the battery. And in that state it
16 looks to be off, typically. For example, you can be working
17 on a document on an airplane, close your notebook, it goes
18 into hibernation, you can go back to your office, open it,
19 and it pops right back to the point -- it restores the
20 hibernation file, and you're right back where you were on the
21 airplane, looking at the same document, the cursor is in the
22 same place.

23 Q. And I guess it would make sense, if you were a
24 police officer and you were going to seize a computer, and
25 you couldn't determine whether it was running because it was

1 either in sleep or hibernation mode, to assume that it was
2 running and deprive it of power. There wouldn't be any harm
3 in doing that if it was actually fully powered off; right?

4 A. That's right. I think I would make that
5 assumption.

6 Q. Can you be a little more descriptive about the
7 consequences if a computer that is running, even if it is in
8 sleep or hibernation mode, is not deprived of power when it
9 is seized by the police. What kinds of things can happen
10 after that that would affect the integrity of the data on
11 that computer?

12 A. Well, if -- let's assume -- and one scenario, the
13 computer never was opened again, and at some point down the
14 road the battery were removed, the only change between its
15 previous working state and the point at which it had the
16 battery removed would be the creation and existence of a
17 hibernation file, which can be quite large, where the machine
18 stores everything that is in memory off to the hard drive.
19 So you could have a very large hibernation file on the disk.

20 Now on the other hand, if that computer's
21 lid is opened sometime after it has gone into hibernation, it
22 is back to where it was when it went into hibernation, and
23 that may have been right in the middle of a process that was
24 changing data on the drive, it might have been in some
25 quiescent state, just logged into a Web page and doing little

1 else. So there could be a variety of activities that could
2 automatically restart once it comes out of hibernation.

3 Q. And by contrast let's just assume, for purposes of
4 this hypothetical, the police seize a computer, it's in
5 hibernation mode running off the battery. And my
6 understanding is it would not take very much battery power.
7 It could run for quite some period of time in hibernation
8 mode before the battery goes dead; right?

9 A. That's right.

10 Q. But let's say it's sitting on a shelf in the
11 police department evidence room, and then eventually the
12 battery just goes dead. The battery is still in the laptop,
13 and it goes dead.

14 Would that event -- the death of the
15 battery -- write anything to any files in the computer?

16 A. I don't know that I can state that for a fact. I
17 don't believe that it would make a difference in most
18 computers.

19 But again, the one change that would have
20 been made to the state of the machine from the time it went
21 into hibernation would be the existence of that large
22 hibernation file.

23 Q. Let's talk, then, specifically about this laptop
24 here. So you take possession of it a week ago Sunday and you
25 make the backups and working copies of it that you described

1 for us.

2 Can you tell us, then, just in general
3 terms, what your next series of work-related steps would be
4 with that hard drive.

5 A. I try to cover all of the major areas of a typical
6 forensic analysis, initially running what is more accurately
7 called an "EnCase report," and that is a fundamental report
8 that tells you about the hardware, the computer, the memory,
9 and also about the hard drive; how big it is, how many
10 sectors it is, all of the things that are good to know even
11 if not sometimes used.

12 I then also moved into disk-based
13 information, checking on Web activity by collecting all of
14 the files. There is a certain type of file in the Windows
15 operating system that records Internet activity. I collected
16 all those files, exported the data from the image, and
17 analyzed that -- I shouldn't say "analyzed," but I collected
18 all that information with an industry-standard tool called
19 "Net Analyzer" that knows how to take apart a DAT file and
20 pull the data out of it.

21 Q. These DAT files are -- D-A-T -- is the extension
22 for the name of the file.

23 Are those the files that you are talking
24 about that store all Web activity on the computer?

25 A. Yes. They are actually called "index.dat." The

1 first name is "index." And on this computer there are about
2 50 of them. Not all of them track Internet activity. The
3 Windows operating system uses DAT files for a number of
4 different purposes.

5 But there is a collection of those DAT
6 files that is specifically devoted to Internet Web access as
7 well as file access and storing cookies from Websites.

8 Q. What is a "cookie"?

9 A. A "cookie" is typically a very small file that is
10 put on your computer -- with your permission or without your
11 permission, for that matter -- by a Website, so that it knows
12 a little bit about who you are and what your browsing habits
13 are. The benefit to the user being the next time you come
14 back to that Website, all it has to do is look for your
15 cookie, and it knows who you are, so you don't have to log
16 in. It may have your password and name and all that.

17 It may also contain a great deal of
18 information about the activity, once you are on that site.
19 For instance, what links did you click on? How did you get
20 there in the first place? Did you type in the name of the
21 Web page or were you transferred there from another Website
22 who had a link? A lot of companies share those kinds of
23 links.

24 So you click on one Web page, and it
25 takes you automatically to another. That could be stored in

1 the cookie, as well.

2 Q. And I imagine from an advertising and marketing
3 perspective, people who -- businesses who may have Websites
4 want to have cookies placed so that they can target e-mail
5 and other information to the people that seem to be
6 interested in them in the first place. Have I got that
7 right?

8 Q. Or even target the ads they put up on the Web
9 page. You know, if the last time you were there you were
10 browsing automobiles, the next time you come in -- it knows
11 you were looking at pickup trucks last time, so it starts
12 putting up the latest deals on pickup trucks on the Website.
13 Yeah, advertisers were a big influence for cookies.

14 Q. What else can you see on these index.dat files?

15 A. The cookies the Websites visited. Although, I
16 have to say I didn't go into a great deal of analysis on
17 this, given the time I had.

18 I collected all the information into a
19 spreadsheet, gave that to you so that you could take a look
20 at it. But I haven't spent a great deal of time going
21 through all the entries to make much sense of them and figure
22 out what story they tell.

23 Q. Let's talk a little bit, if we could while we
24 still have some time this afternoon, about the particular
25 time stamps on some of the data that you did look at on this

1 forensic image.

2 And the first area that I am interested
3 in are some entries that are reflected in Detective Page's
4 report that seem to show, before we looked at it, that there
5 had been some activity with respect to this computer on
6 July 8, 2008; is that right?

7 A. Yes.

8 Q. And the significance of that, you can understand,
9 was that the police came in possession of his computer on
10 July 3rd, and there is some activity on July 8th; is that
11 right?

12 A. That's right. I found that curious because the --
13 there was activity on July 2nd. The last activity, I think,
14 was about 4:30 in the afternoon.

15 Then there was a gap until July 8, and
16 then there was another flurry of activity, including some
17 entries in the index.dat file for Web access. There was a
18 Google entry. And also including a bunch of file activity on
19 the hard drive that -- I think there were about 350 files
20 that had date and time stamps for July 8th, including some
21 deleted files.

22 Q. Let's go back and talk about the July 2nd
23 activity, first, in sequence. In Detective Page's report,
24 which is in evidence in this proceeding, there is some
25 indication that a number of files had a time stamp called

1 "Last Access," and there were a number of them in that report
2 that you were given that all had a last access time stamp of
3 a couple of minutes before midnight on July 2nd, 2008. Did
4 you look at those files?

5 A. I did.

6 Q. Even given that time stamp of almost midnight on
7 July 2nd, why is it that you believe that the last activity
8 on July 2nd was earlier -- was closer to 4:30?

9 A. Well, I looked at two different kinds of date and
10 time stamp data. I looked at the Windows metadata, which is
11 the time activity associated with the file that is stored on
12 the hard drive. That was straightforward -- you know, 4:40
13 or so in the afternoon.

14 When I was looking at the Internet
15 activity, however, there were some entries that said 11:40 at
16 night, but the Internet activities are based on what's called
17 "UTC," universal time -- universal coordinated time, which is
18 similar to Greenwich Mean Time. And Arizona is seven hours
19 behind UTC. So that corresponds to the Windows metadata of
20 4:40 in the afternoon.

21 Q. Would it be your professional opinion that, with
22 regard to these particular files that you were directed to
23 look at, that notwithstanding the fact that they may appear
24 to be time stamped at nearly midnight, that in reality that
25 activity took place before 5:00 in the afternoon?

1 A. Yes. And it's easy to be misled on that. But
2 when looking at the two different types of data, it makes a
3 great deal of sense, because they were the same time to the
4 second, seven hours off.

5 Q. Now, let's move ahead to July 8, considering that
6 that is a number of days after the police took possession of
7 this laptop.

8 What did you find about July 8 in terms
9 of the time of this activity and, again, describing what it
10 was that you were seeing on the forensic image that related
11 to activity on July 8?

12 A. Again, I have to preface my comments with I
13 haven't spent a great deal of time analyzing that data. I
14 have been collecting more than analyzing.

15 But I do know the flurry of activity
16 happened at about 3:50 in the morning -- sometime between
17 3:40 and 4:00 in the morning. And again, that included
18 deletion of files and other file activity that created dates
19 and time stamps of the 8th at 3:40 in the morning.

20 Q. Now, in your opinion, would the activity that you
21 are seeing recorded on the forensic image of 3:40 or 3:50 in
22 the morning on July 8 be consistent with the battery simply
23 dying?

24 A. No. It would be consistent with the machinery
25 starting itself and coming out of hibernation.

1 Q. Coming to life?

2 A. Yes. Or perhaps turned on, I should say. But I
3 think it was hibernation.

4 Q. Let's assume, again, a couple of hypothetical
5 circumstances. Let's say that when the computer was taken by
6 the police on July 3, it was running in an unspecified state,
7 perhaps sleep or hibernation mode, and the battery was not
8 removed, and it and was taken into police custody. And
9 wherever it was on July 8, for some reason or another,
10 someone opened the lid.

11 First of all, what effect would that have
12 on the computer?

13 A. It would have a number of possible effects. I
14 can't really speculate without taking a closer look at the
15 data, but some of the data I did look at was the hibernation
16 file, because that ties into this whole question. And I
17 found three different hibernation files that the operating
18 system uses, and two of them did have July 8 date stamps, so
19 that's why I am speculating that the computer came out of
20 hibernation, read those files back into memory on July 8.

21 Q. Now, going backwards, would the computer have, on
22 its own, gone from, say, sleep mode or fully active and
23 wide-awake state into hibernation without someone doing
24 something to it?

25 A. No, it would take user intervention.

1 Q. So the chances are if it was coming out of
2 hibernation -- is it fair to say it was likely in hibernation
3 when it was collected?

4 A. That would be what I would say, yes.

5 Q. And other than somebody physically opening a lid,
6 is there anything else that you can think of that could
7 happen to that computer that could cause it to come alive and
8 start writing?

9 A. I have never heard of that happening, because
10 there are no controls on the computer that are not under the
11 lid, typically. I would have to look at this model
12 specifically. But your power buttons, sometimes a keystroke
13 can bring it out of hibernation -- just hitting the space
14 bar -- sometimes you have to touch the power button, but that
15 is all under the lid.

16 Q. Can those kinds of computers go into hibernation
17 with the lid open?

18 A. Yes. You can set some computers to go into
19 hibernation after a certain amount of inactivity.

20 Q. Would it be consistent with industry standards to
21 seize the computer with the lid open and not close it? Just
22 leave it open?

23 A. Once it's in custody?

24 Q. Yes.

25 A. If it was properly deprived of power, it wouldn't

1 matter one way or the other.

2 Q. If you had the battery in it, would it be risky to
3 leave it in storage on a shelf someplace with the lid open?

4 A. Yes, I would say so. Because if you've got a
5 blank screen, that just doesn't mean that the machine is
6 turned on. The only way to ensure that it is not is to pull
7 the battery, if it is in hibernation.

8 Q. One final area on this point. When -- based on
9 what you saw in this forensic image, when the machine came
10 alive and started to write, does that in any way overwrite or
11 damage other data that was pre-existing on that drive?

12 A. It's certainly possible. Again, I haven't looked
13 closely enough to know what the software is -- you know, what
14 comprises those 350 files.

15 If it were Norton Antivirus or if it were
16 a Windows defragmentation housekeeping program that began
17 running, yes, spoliation could occur to a large degree.

18 Q. You are not at a point yet where you can express
19 an opinion about that?

20 A. I cannot.

21 MR. SEARS: Thank you.

22 I think this might be a good point when
23 the Court is inclined to break for the day.

24 THE COURT: Timing is excellent.

25 MR. SEARS: Thank you.

1 THE COURT: We will recess, then.
2 Mr. Cardwell, you may step down.
3 We will resume on Thursday, the 15th of
4 January, at nine o'clock in the morning.

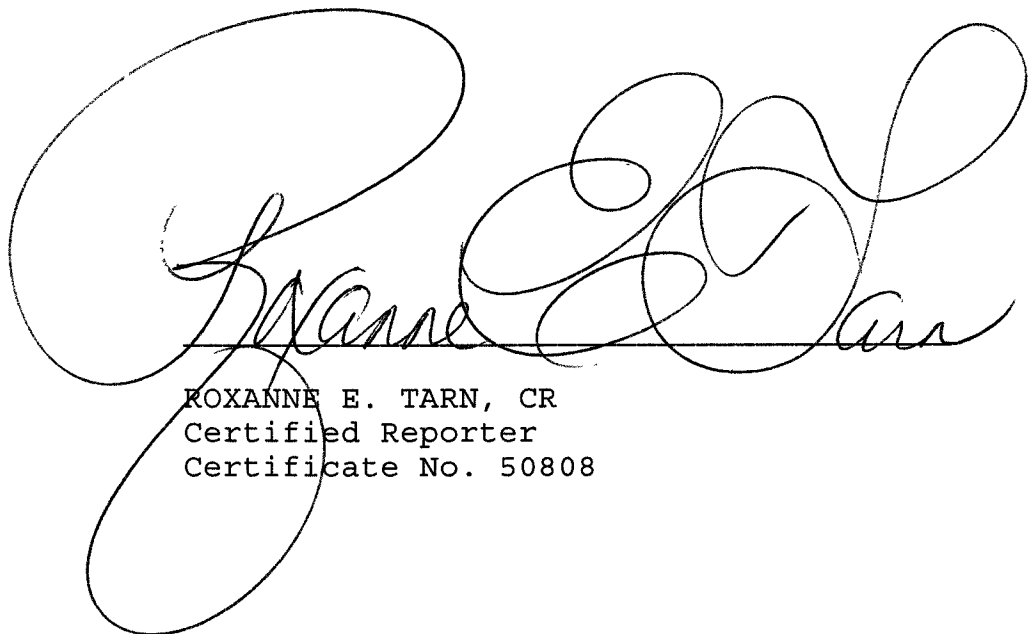
5 (Whereupon, these proceedings were concluded.)

6 ***o0o***
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C E R T I F I C A T E

I, ROXANNE E. TARN, CR, a Certified Reporter
in the State of Arizona, do hereby certify that the foregoing
pages 1 - 21 constitute a full, true, and accurate transcript
of the proceedings had in the foregoing matter, all done to
the best of my skill and ability.

SIGNED and dated this 21st day of August,
2009.



ROXANNE E. TARN, CR
Certified Reporter
Certificate No. 50808